Zen and the Art of Threat Intelligence and Attribution

Jennifer Kolde
Principal Threat Intelligence Analyst
Mandiant

Obligatory Background Slide

- Jennifer Kolde

  ~ >1 year at Mandiant

  ~ 6 years (total) specifically tracking targeted threats

  ~ 10 years (total) dealing with targeted threats (directly or indirectly)

  15+ years in IT / IT security

- Expertise thanks to:
  - I've done this for a long time.
  - I've made most of the mistakes I'm going to describe to you.

What to Expect

- What is Threat Intelligence and Why is it Important?
- What is Attribution and Why is it Important?
- What is a Threat Group?
- What is an Indicator?
- What is Badtribution?
- The Top 10 Reasons Badtribution Happens

What is Threat Intelligence?

- Most people can't tell you
- Some vendors define it by what it "does"
- Doesn't tell you what it IS

Reasonable Definition

- “Threat intelligence is **evidence-based knowledge**, including context, mechanisms, indicators, implications and actionable advice, **about an existing or emerging menace** or hazard to assets **that can be used to inform decisions** regarding the subject's response to that menace or hazard.”

  - Gartner Research

Simplified

- Evidence-based knowledge
- About an existing or emerging menace
- That can be used to inform decisions
- “Know your enemy”

Obligatory picture of Sun Tzu

Why is Threat Intelligence Important?

- **“…that can be used to inform decisions…”**
- Network defenders are bombarded with alerts and incidents on a daily basis
- Threat Intelligence allows you to defend your network:
  - Faster
  - More efficiently
  - More effectively

Use Threat Intelligence To…

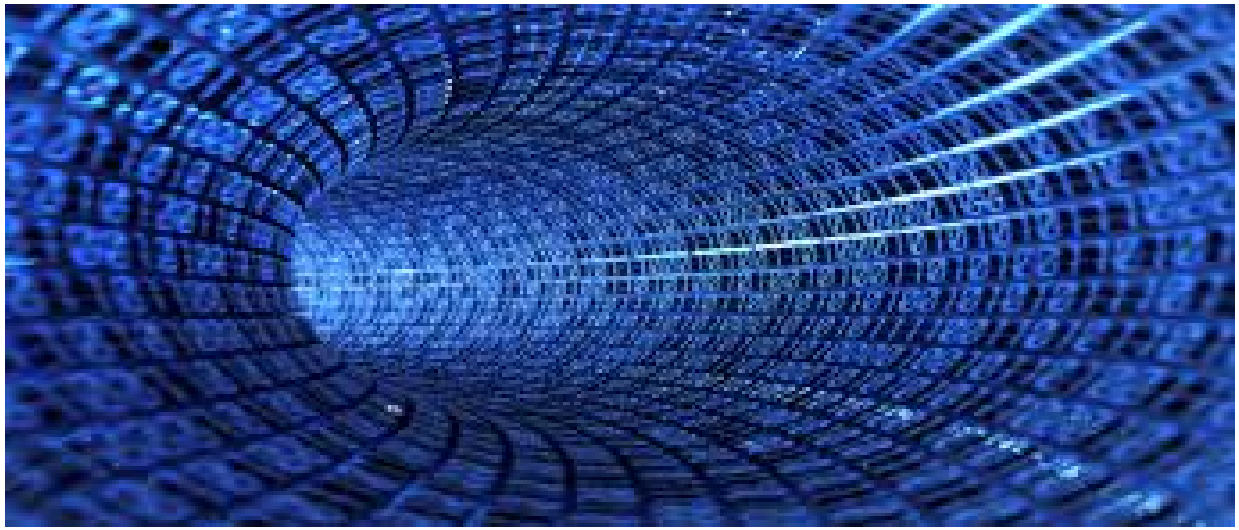
- Build up knowledge of attacks against your organization
- Leverage to triage future incidents
  - Prioritize response
  - Anticipate attacker tactics, techniques, and procedures (TTPs)
  - Invest wisely based on known TTPs

What is Attribution?

- Definition #1: determining the identity of a threat group
- “Threat Group X is really Organization Y”

What is Attribution?

- Definition #2: associating specific activity with a particular threat group.
- Being able to state that Threat Group X did Y.
- …even if you don't know who Threat Group X is.



Why is Attribution Important?

- If you believe threat intelligence (“know your enemy”) is important, then…
  - …you need to know who your enemy is.
- Attribution literally defines your enemy.
- If key benefits of threat intelligence are:
  - more rapid identification of your enemy
  - anticipation of your enemy’s moves (TTPs)
- …then it’s important to get the attribution part (the definition) right.

For Example…

- Indicators are attributed to threat groups.
- If you get this wrong…
  - …then you mischaracterize the threat
- Examples:
  - False positive
    - Mis-identifying activity from Group A as Group B
    - Mis-identifying lower-risk activity as higher-risk activity
  - False negative
    - Mis-identifying higher-risk activity as lower-risk activity
    - Failing to identify activity as malicious

What is a Threat Group?

- I bet you thought you knew the answer to this.
- Most people can name threat groups but can't explain what they are
  - "Comment Crew"
  - "Shady Rat"
  - "Luckycat"
  - "Gh0stNet"

Option #1

- A threat group is a **defined organization or group of individuals** responsible for a set of threat activity.
- Matches our first definition of “attribution”.
- Defines the group, then attempts to associate with activity.

Option #2

- A threat group is a set of threat actors responsible for **an interrelated set of activity**
- Matches our second definition of “attribution”.
- Defines the activity, then attempts to trace it back to a group.
- Activity still carried out by people…we just may not know who they are (yet).

What is an “interrelated set of activity”?

- In short…a set of TTPs and their associated indicators.
- Hackers are people.
- TTPs are the stuff they do when they hack.
- People have habits, comfort zones, and routines…
- TTPs are a way to recognize an individual hacker (or group) by what they DO, even if you don’t know who they ARE.

What is an Indicator?

- TTPs can be:
  - Vague
  - Concrete
- Concrete TTPs are easier to work with, correlate, and monitor for. They are:
  - Specific
  - Atomic
  - Unique (ideally)

For Example…

- Bad Stuff happens on your network.
- You find 13 instances of malware and utilities used to commit the badness.
- The malware communicates with 7 DNS domains.
- The stuff the malware collected and packaged up was sent to three external IP addresses.

Congratulations! Those data points are the beginnings of a threat group (or groups…)

Not All Indicators are Created Equal

- Indicators may vary in:
  - **uniqueness** (how likely is it that this indicator is only used by one threat actor / threat group?)
  - **proximity** (how "close" – in time or space – was this indicator the actual Bad Stuff?)
  - **fidelity** (how reliable is your information? Did you see it happen, did someone else tell you about it, or did you read about it on teh interwebz?)

- Determining whether indicators are related – and with what degree of confidence – is the "art" of attribution

Primary Indicators

- Primary indicators are your “Ground Zero”.
- They are raw data, directly involved in the Bad Stuff that occurred[1]:
  - The email address that sent the spear phish
  - The IP address the email was sent from
  - The malware attached to the email

[1] Caveat: there is always a caveat.

Secondary+ Indicators

- Secondary indicators bear some relation to primary indicators[1].
  - A DNS domain embedded in the malware attached to the email
- You can also have tertiary (and beyond) indicators:
  - The embedded DNS domain resolved to a specific IP address
  - Another domain resolved to the same IP that the domain from the malware…and so on.
- Indicators get **less reliable** the farther away you get from Ground Zero.

[1] Caveat: see previous caveat.

Basic Steps of Attribution

- To build a threat group (and to start building threat intelligence):
  - Find evil.
  - Find concrete things associated with evil.
  - Ensure the concrete things are part of the same evil.
  - Call it something.
- See when / whether those indicators appear elsewhere.
- Lather, rinse, repeat.

Also…

Be prepared to be wrong.

What is Badtribution[1]?

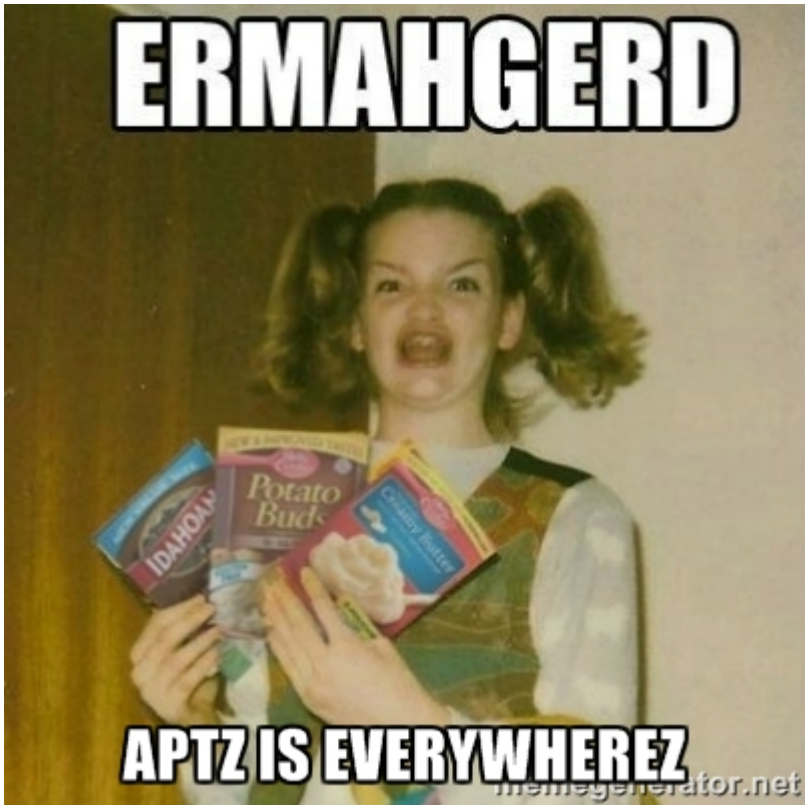
- Basically…getting it wrong.
- Faulty analysis that leads to an incorrect assessment and ultimately to flawed threat intelligence.

- Well….
- Technically, faulty analysis is just “bad attribution”.

[1] Note: much debate over the origin of this term. Many people want to be credited with this cleverness. I honestly don’t know who came up with it.

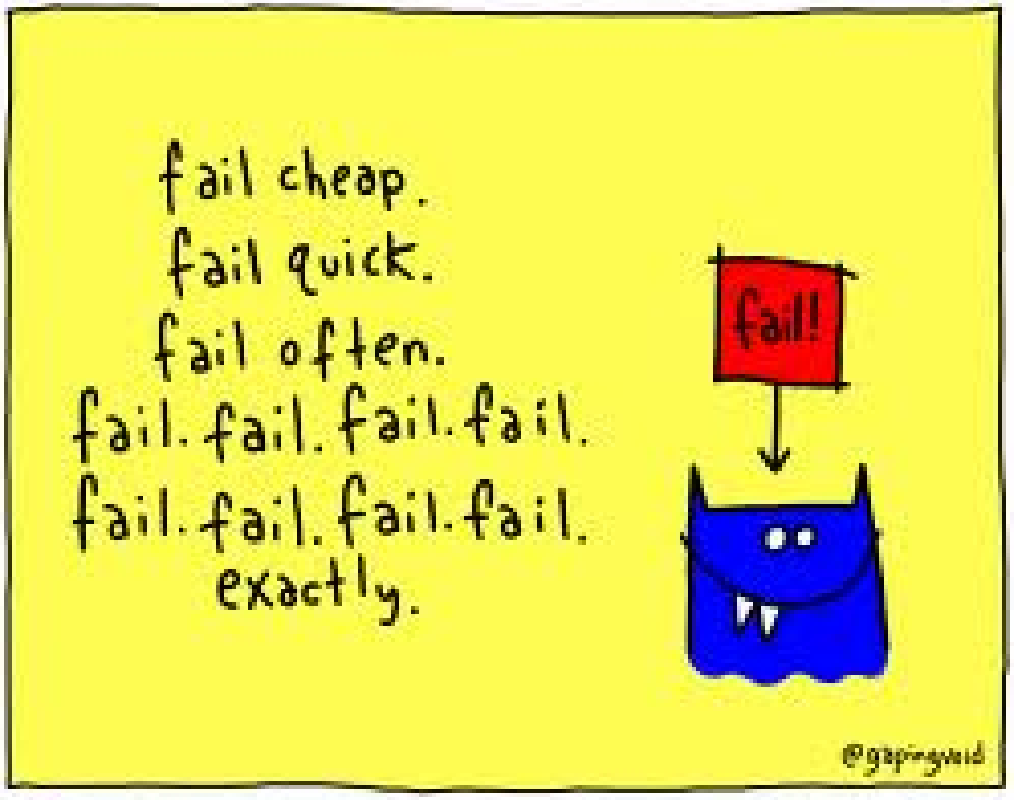
True Badtribution is…

- …a spectacular failure of the analytical process.
- Really fun to say.



Why Badtribution Exists…

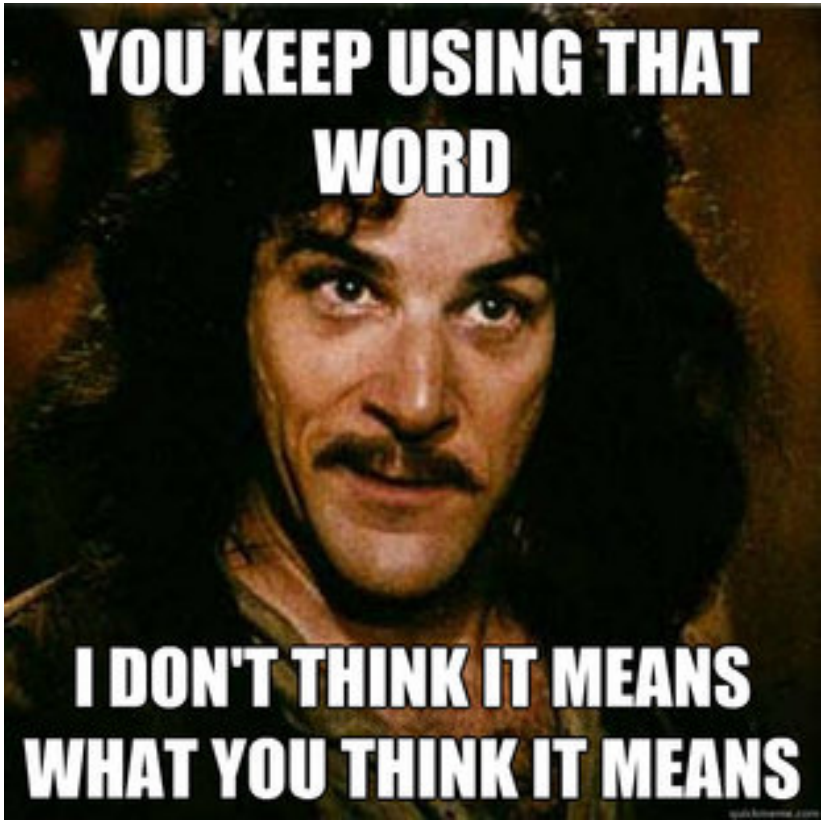
- …or, “The Top 10 Reasons Threat Intelligence Fails”



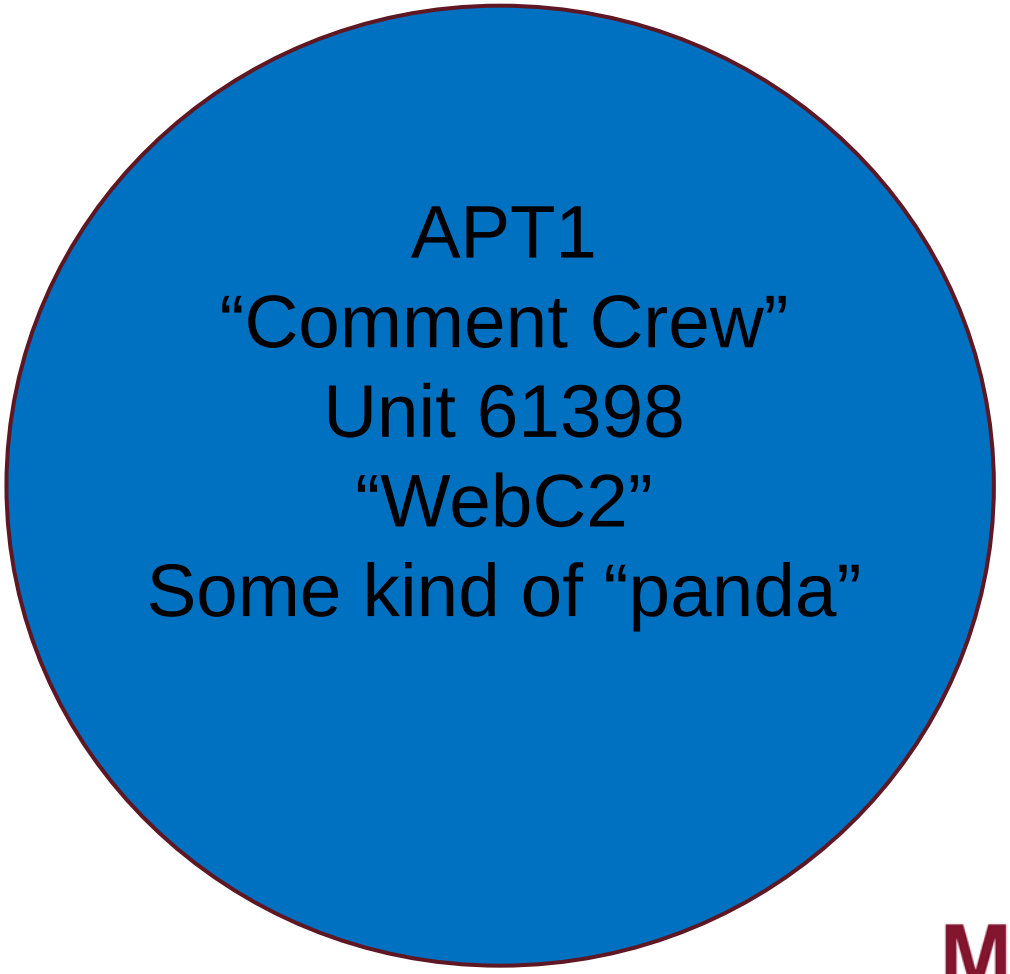
1. We Have No Idea What We're Talking About

- The "Threat Intelligence Community"[1] tosses terms around like nobody's business.
- Everyone assumes we're talking about the same thing…
  - …and that we all know what we're talking about.

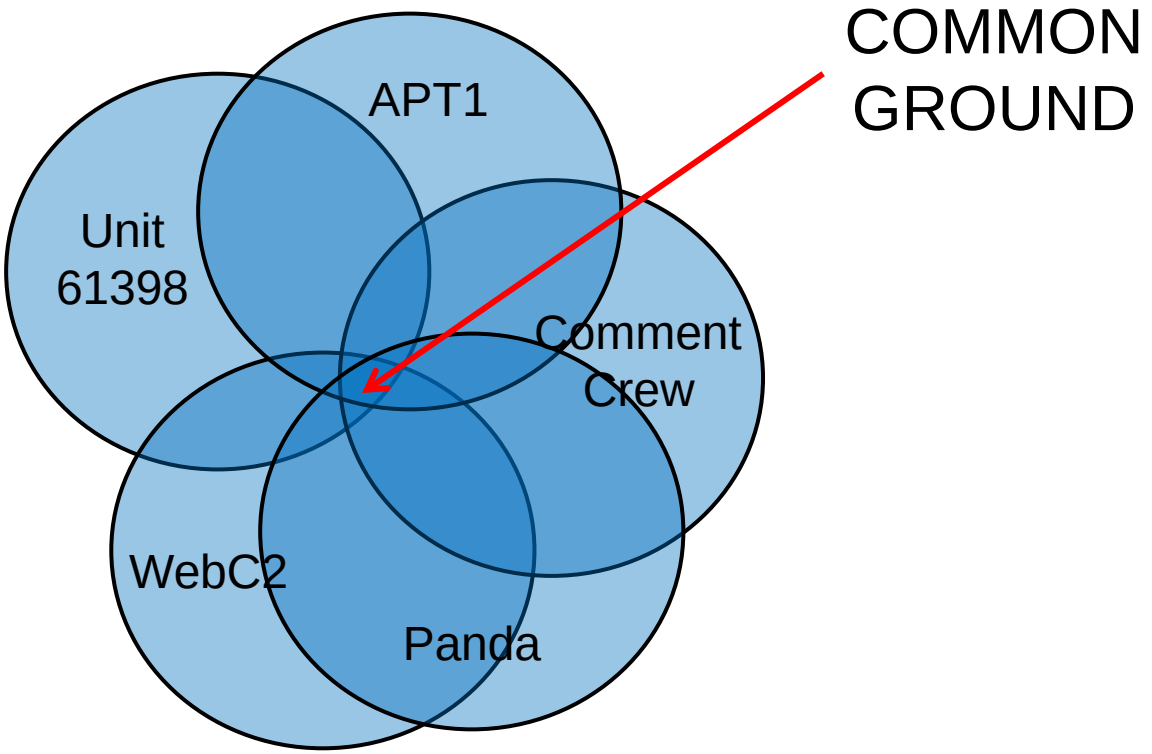
[1] This is an undefined term.



What We Think We're Talking About



What We're Really Talking About



Exaggerated for effect, but you get the idea.

2. Infosec People are not Intelligence Analysts (and vice versa)

- Information Security is its own distinct discipline.
- So is Intelligence Analysis.
- It’s really, really hard to find people with an understanding of both.

3. Failure to Account for Reliability of Data

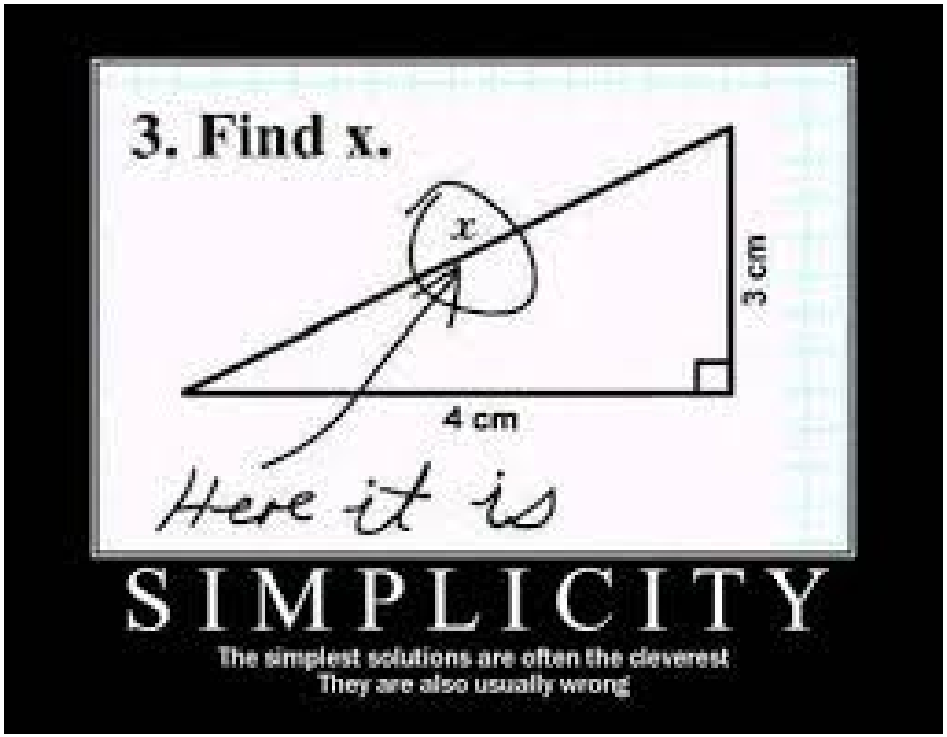
- Typically done by technical personnel trying to do intelligence analysis.
- In the intelligence community, this is known as “confidence”.
- Technical personnel tend to think more in black and white terms.
- Mistaken reliance on low confidence data can lead to errors.

4. Failure to Understand the Technical Details

- Typically made by intelligence analysts trying to make sense of technical data.
- Lack of precise understanding of technical concepts or processes leads to errors.
  - Failure to interpret data correctly.
  - Failure to account for alternate explanations.
  - Failure to recognize significance of certain data.

5. Oversimplfication

- …is what both of the above errors can lead to.
- Humans like simple explanations
- The fundamental language of computers is binary.
  - Technical people in particular don't always deal well with gray areas.
- The simplest explanation is not always correct.

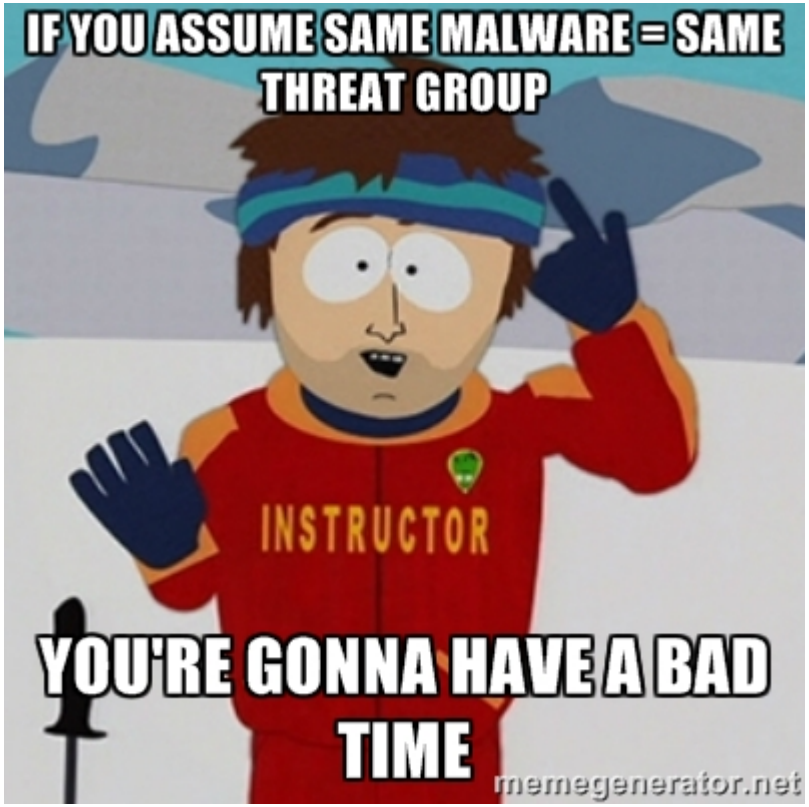


6. Confusing Fact with Opinion

- …or worse, speculation.
- Good analytical writing – and good analysis – clearly separates:
  - What is known
  - What is assumed or theorized (no matter how "likely" or "possible")
- A lot of written badtribution conflates the two.
- A lot of badtribution gets done by reading someone else's opinion and believing it as fact.

7. Assuming that Same X == Same Y

- A form of oversimplification
- Applies to any number of X, where X is a thing and Y is usually a threat group



8. Time is not on Your Side

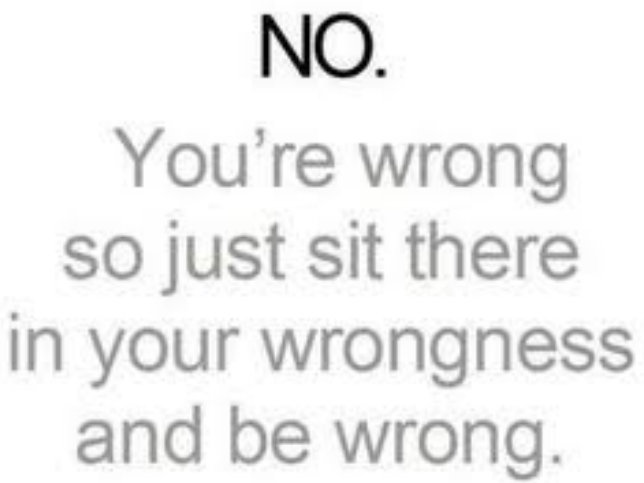
- Back in the good old days, it was enough to:
  - Determine something was bad.
  - Identify the other bad things it was linked to.
  - Call it a day.
- Now…we need to know WHEN something was bad.

9. It's Hard to Account for Human Activity

- We expect indicators and data to have direct correlations and relationships
- Those data points represent activity carried out by people
- People and relationships change constantly
- "Who" is involved in malicious activity may be more complicated than we think

10. There is Always Something You Haven't Thought Of

- No matter how thorough you are…
- …there will be something that you miss.
- None of us can know everything
- Be prepared to re-evaluate and revise your analysis



So What?

- By identifying and linking **indicators** with associated **activity**…
- …**attribution** defines what we call **threat groups**.
- For Threat Intelligence to have value, it must have reliable attribution.
- Attribution is hard, and there are any number of ways it can go wrong.
- Greater focus on identification and analysis of threat group activity is a Good Thing.
- Analysts (and those relying on their products) must be aware of pitfalls and view “threat intelligence” with a critical eye.

THANKS FOR YOU ATTENTION.
ANY QUESTION ?
DIYLOL.COM